UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/276,233	03/25/1999	TALAL G. SHAMOON	07451.0011-0	1836

22852 7590 02/10/2005

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER	
SANTOS, PATRICK J D	
ART UNIT	**PAPER NUMBER**
2161	

DATE MAILED: 02/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/276,233	SHAMOON ET AL.	
	Examiner	Art Unit	
	Patrick J Santos	2161	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,22 and 26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,22 and 26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Examiner acknowledges that Applicant has elected Group I, Claims 1-7, 22, and 26 without traverse.

Drawings

2. Examiner withdraws objections to drawings set forth in the previous Office Action.

Information Disclosure Statement

3. In the previous Office Action, the information disclosure statements received August 16, 1999 and December 20, 2001 were both objected to under 37 CFR 1.98(a)(2) for not including a copy of the references. Examiner has since received copies of the references, and withdraws objection.

Specification

4. In the previous office action, the specification was objected to under 37 CFR 1.72(b) for not including an abstract. Examiner has since received the abstract.

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Regarding Claims 1-7 and 22, Examiner notes means plus function language in independent Claim 1. As per the two prong test as set forth in MPEP 2181, claim language will be interpreted as per 35 U.S.C. 112, paragraph 6.

7. Claims 1 and 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over the publication, "Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video", by Spanos, et al., as published by the "Proceedings of the Fourth ACM International Conference on Computer Communications and Network," September 1995, (hereafter Spanos '95), in view of the publication, "Applied Cryptography", by Schneier, published by John Wiley and Sons, 1996 (hereafter Schneier '96).

Since the Spanos '95 paper relies on the reader having detailed knowledge of the internals of the DES encryption algorithm, Examiner uses Schneier '96 both to explicate DES as referred to in Spanos '95 and also to disclose the key transfer limitations in the claims.

Claim 1:

Regarding Claim 1, Spanos '95 discloses a method of encrypting and decrypting MPEG video data on an MPEG player. Specifically, Spanos '96 discloses: a streaming media player (Spanos '95: Section Titled, "4. Aegis Performance", p. 4, col. 2, lns. 43-45) providing content protection and Digital Rights Management (DRM) (Spanos '95: Section Titled, "3. Aegis Overview", p. 3, col. 2, lns. 15-43) including:

- a port configured to receive a digital bit stream (Spanos '95: Section Titled, "4. Aegis Performance", p. 4, col. 2, lns. 43-45 – note MPEG players of necessity have an input to receive a digital bit stream);
- the bit stream includes content that is encrypted in part (Spanos '95: Section titled, "3. Aegis Overview", p. 3, col. 2, lns. 15-43 – note the encryption of only the I-frames); and

- a control arrangement (Spanos '95: Section Titled, "4.3 Our Algorithm", p. 223, col. 2, lns. 40-41 – note MPEG player encoders and decoders read on a control arrangement).

Additionally, Spanos '95 explicitly discloses the use of the DES algorithm to encrypt the bit stream (Spanos '95: Section Titled, , "3. Aegis Overview", p. 4, col. 1, ln. 30 to col. 2, ln. 3). However, Spanos '95 does not explicitly describe the DES algorithm, Examiner provides Schneier '96 to describe how DES reads on the remainder of the claim limitations.

Schneier '96 discloses the DES algorithm. Specfically, Schneier '97 discloses:

- control information for controlling use of the content, including at least one key suitable for decryption of at least a portion of the content (Schneier '96: Section Titled, "12.2 Description of DES", p. 270, lns. 5-13 – note description of the key);
- the control arrangement includes means for decrypting the encrypted portion of the content (Schneier '96: Section Titled, "12.2 Description of DES", Subsection Titled, "Decrypting DES", p. 277, lns. 11-22).

Furthermore, Schneier '96 discloses key transfer. Specifically, Schneier '96 discloses:

- the bit stream includes a secure container including the control information which includes the key (Schneier '96: Section Titled, "8.3 Transferring Keys", p. 176, lns. 38-43 – note that Schneier '96 discloses "key-encryption keys" to encrypt "data keys" that may be transferred over the communications channel);
- the control arrangement includes means for opening secure containers and extracting cryptographic keys (Schneier '96: Section Titled, "8.3 Transferring Keys", p. 176, lns. 38-43).

It would have been obvious to a person having ordinary skill in the art to apply the key transfer of Schneier '96 to the encrypted MPEG player of Spanos '95. The motivation to combine is suggested by Schneier '96 which discloses the desirability of not transmitting a data key in the clear over a communications line (Schneier '96: Section Titled, "8.3 Transferring Keys", p. 176, lns. 34-37).

Claim 6:

Regarding Claim 6, Spanos '95 and Schneier '96 in combination disclose all the limitations of Claim 1 (supra). While, Spanos '95 and Schneier '96 in combination disclose use of MPEG-1 and MPEG-2 (Spanos '95: Section Titled, "4. Aegis Performance", p. 4, col. 2, lns. 43-45). However, Spanos '95 and Schneier '96 in combination do not explicitly disclose substituting MPEG-4 data for MPEG-1 or MPEG-2 data.

Examiner takes official notice on MPEG-4 data.

It would have been obvious to a person having ordinary skill in the art to substitute MPEG-4 data for the MPEG-1 and MPEG-2 data. MPEG-4 supports Groups of Frames and Spanos '95 and Schneier '96 disclose that the Aegis video data encryption/decryption approach is applicable to MPEG data that supports Groups of Frames (Spanos '95: Section Titled, "3. Aegis Overview", p. 3, col. 1, lns. 20-29).

8. Claims 2-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spanos '95 and Schneier '96 in view of U.S. Patent No. 5,875,303 issued to Huizer et al. (Huizer '303).

Claim 2:

Regarding Claim 2, Spanos '95 and Schneier '96 in combination disclose all the limitations of Claim 1 (supra). Additionally, Spanos '95 and Schneier '96 in combination

disclose: in which the digital bit stream includes at least two sub-streams including compressed information (Spanos '95: Section Titled, "3. Aegis Overview", p. 3, col. 1, lns. 16-29 – MPEG reads on substreams and compressed information).

However, Spanos '95 and Schneier '96 in combination do not explicitly disclose: wherein the player further includes:

- a demux designed to separate and route the sub-streams;
- a decompression unit configured to decompress at least one of the sub-streams, the decompression unit and the demux being connected by a pathway for the transmission of information; and
- a rendering unit designed to process decompressed content information for rendering.

Huizer '303 discloses the Philips (TM) CDi (TM) media streaming player. Specifically, Huizer '303 discloses: wherein the player further includes:

- a demux designed to separate and route the sub-streams (Huizer '303: Fig. 6, item 71 (demux); col. 6, lns. 60-65);
- a decompression unit configured to decompress at least one of the sub-streams, the decompression unit and the demux being connected by a pathway for the transmission of information (Huizer '303: Fig. 6, items 71 (demux) and 5 (decoder which in the context of CDi and MPEG read on a decompression unit) connected by items 72, 74, and 73); and
- a rendering unit designed to process decompressed content information for rendering (Huizer '303: col. 6, lns. 55-57).

It would have been obvious to a person having ordinary skill in the art to apply the configuration of Huizer '303 to the MPEG player of Spanos '95 and Schneier '96 in

combination. The motivation to combine to include a demultiplexer, a decompression unit, and a rendering unit as taught by Huizer '303 is on the basis that these parts are integral and necessary to a streaming media player such as the MPEG player of Spanos '95 and Schneier '96 in combination.

Claim 3:

Regarding Claim 3, Spanos '95, Schneier '96, and Huizer '303 in combination disclose all the limitations of Claim 2 (supra). Additionally, Spanos '95, Schneier '96, and Huizer '303 in combination disclose: a stream controller operatively connected to the decompression unit (Huizer '303: Fig. 6, item 75 with items 71, 72, 73, 74, and 5), the stream controller including decryption functionality configured to decrypt at least a portion of a sub-stream and pass the decrypted sub-stream to the decompression unit (Spanos '95: Section Titled, "3. Aegis Overview", p. 4, col. 1, ln. 30 to col. 2, ln. 3 – note that DES is integrated into the media player).

Claim 4:

Regarding Claim 4, Spanos '95, Schneier '96, and Huizer '303 in combination disclose all the limitations of Claim 2 (supra). Additionally, Spanos '95, Schneier '96, and Huizer '303 in combination disclose: a path between the control arrangement (Huizer '303: Fig. 6, item 4, a path to the control channel from a remote server) to pass at least one key to the stream controller for use with the stream controller's decryption functionality (Schneier '96: Section Titled, "8.3 Transferring Keys", p. 176, lns. 38-43).

Claim 5:

Regarding Claim 5, Spanos '95, Schneier '96, and Huizer '303 in combination disclose all the limitations of Claim 4 (supra). Additionally, Spanos '95, Schneier '96, and Huizer '303 in

combination disclose: a feedback path from the rendering unit to the control arrangement to allow the control arrangement to receive information from the rendering unit regarding the identification of objects which are to be rendered or have been rendered (Huizer '303: col. 5, lns. 50-60).

9. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spanos '95 and Schneier '96 in view of U.S. Patent No. 4,649,233 issued to Bass et al. (hereafter Bass '233).

Claim 22:

Regarding Claim 22, Spanos '95 and Schneier '96 in combination disclose all the limitations of Claim 1 (supra). However, Spanos '95 and Schneier '96 in combination do not explicitly disclose: wherein the control arrangement includes tamper resistance.

Bass '233 discloses: wherein the control arrangement includes tamper resistance (Bass '233: col. 4, lns. 45-51).

It would have been obvious to a person having ordinary skill in the art to apply the tamper resistance of Bass '233 to the control arrangement of Spanos '95 and Schneier '96 in combination. The motivation to combine is suggested by Bass '233 which discloses the advantage of additional security in the event of physical hacking attempts (Bass '233: col. 4, lns. 45-51).

10. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spanos '95 and Schneier '96 in view of U.S. Patent No. 5,694,332 issued to Maturi (Maturi '332).

Regarding Claim 7, Spanos '95 and Schneier '96 disclose all the limitations of Claim 1 (supra). However, Spanos '95 and Schneier '96 do not explicitly disclose: the digital bit stream is encoded in MP3 format.

Maturi '332 teaches the use of an arbitrary audio stream (Maturi '332: p. 3, Fig. 2 and supporting text) and is explicitly inclusive of MP3 data (Maturi '332: col. 3, lns. 42-46).

It would have been obvious to a person having ordinary skill in the art to substitute the MP3 decoder of Maturi '332 for the MPEG decoder in the Spanos '95 and Schneier '96 combination in order to create an MP3 audio standards compliant implementation and thus create a more diverse market for the invention. Futhermore, Spanos '95 and Schneier '96 disclose the success in applying security algorithms in encrypting audio data (Spanos '95: Section Titled, "3. Aegis Overview", p. 3, col. 2, lns. 3-12).

11. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spanos '95, in view of publication "How Plug-Ins 'Plug In,'" by Mark R. Brown, 1996 (Brown '96), as referenced in the IDS received 12 May 2003, and in further view of U.S. Patent No. 5,794,038 issued to Stutz et al. (Stutz '038).

Claim 26:

Regarding Claim 26, Spanos '95 discloses: a method of rendering a protected digital bit stream (Spanos '95: Section Titled, "4. Aegis Performance", p. 4, col. 2, lns. 43-45) including:

- receiving the protected digital bit stream (Spanos '95: Section Titled, "4. Aegis Performance", p. 4, col. 2, lns. 43-45 – note the input into the player is the selectively encrypted MPEG video stream);
- passing the protected digital bit stream to a media player (Spanos '95: Section Titled, "4. Aegis Performance", p. 4, col. 2, lns. 43-45).
- a first module decrypting at least a portion of the protected digital bit stream (Spanos '95: Section Titled, , "3. Aegis Overview", p. 4, col. 1, ln. 30 to col. 2, ln. 3); and

- a second module decompressing at least a portion of the decrypted digital bit stream (Spanos '95: Section Titled, "4. Aegis Performance", p. 4, col. 2, lns. 43-45 – note a media player decompresses a digital bit stream for rendering);

However, Spanos '95 does not explicitly disclose:

- the media player reading first header information identifying a plug-in used to process the protected digital bit stream, the first header information indicating that a first plug-in is required;
- the media player calling the first plug-in;
- the media player passing the protected digital bit stream to the first plug-in;
- the first module is implemented in the first plug-in;
- the first plug-in reading second header information identifying a second plug-in necessary in order to render the decrypted digital bit stream;
- the first plug-in calling the second plug-in;
- the first plug-in passing the decrypted digital bit stream to the second plug-in;
- the second module is implemented in the second plug-in;
- the second plug-in passing the decrypted an processed digital bit stream to the media player; and
- the media player enabling rendering of the decrypted and processed digital bit stream, whereby the first plug-in may be used in an architecture not designed for multiple stages of plug-in processing.

Brown '96 teaches use of a plug-in embodiment for streaming media applications (Brown '96: p. 18, lns. 11-20). However, Brown '96 does not explicitly teach: the separation of functionality across multiple plug-ins.

Finally Stutz '038 teaches the separation of functionality across multiple plug-ins (Stutz '038: col. 30, lns. 3-38)

It would have been obvious to a person having ordinary skill in the art to implement the first and second modules of Spanos '95 into plug-ins as as disclosed by Brown '96, and further to create an embodiment in which functionality is separated across multiple plug-ins as disclosed by Stutz '038.

The motivation to implement the first and second modules of Spanos '95 in a plug-in embodiment is explicitly taught by Brown '98 as follows: "Plug-ins are a godsend for applications developers, who can extend the utility of existing products into the burgeoning Internet market by developing a quick and easy NETSCAPE (TM) plug-in that reads existing data files, instead of developing a whole new product. Not only does this save developers time and effort, it lets them ride into a huge market riding on the coattails of NETSCAPE (TM) ..." (Brown '96: p. 18, lns. 11-20). Thus, a plug-in embodiment of the first and second modules of Spanos '95 would extend the market reach of the combination.

The motivation to implement the first and second modules of the Spanos '95 and Brown '96 combination by separating the decryption and decompression into a first and a second plug-in occurs from a desire to reduce run-time overhead (Stutz '038: col. 7, lns. 15-27). Specifically, when a software service, such as decrypting and decompressing a bit stream, is dependent on multiple possible embodiments, such as MPEG-4 and MP3, a standard approach is

to create a first object responsible for determining which embodiment is required, and then to delegate processing to a second specializing object. In this way, an object that is not required is never instantiated, and thus does not create run time overhead. As applied to the aforementioned example, if the bit stream was an MPEG-4 bitstream, the first module would determine that a MPEG-4 decrypting/decompression object would have to be instantiated, would then instantiate it, and then would delegate processing to it. In doing so, any other modules not required would not be instantiated in the first place, and thus would save run-time resources. Thus it would have been desirable and obvious to apply the Stutz '038 teaching of separating the first and second modules of Spanos '95 and Brown '96 in combination into a corresponding first and second plug-in.

Response to Arguments

12. Applicant's arguments with respect to Claims 1-7, 22, and 26 have been considered but are moot in view of the new grounds of rejection.

Conclusion

13. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Tang, Lei, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently", 1997, Proceedings of the Fourth ACM International Conference on Multimedia, pp. 219-229.
- Gong, Kevin L., Lawrence A. Rowe, "Parallel MPEG-1 Video Encoding", September 1994, report published by the Berkeley Multimedia Research Center http://bmrc.berkeley.edu/research/publications/1994/120/msreport-fin.html, 27 pages.
- ___, "Key Management Using ANSI X9.17", April 27, 1992, Published by the U.S. Department of Commerce as Federal Information Processing Standard Publication 171.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Patrick J Santos whose telephone number is 571-272-4028. The examiner can normally be reached on M-F 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Safet Metjahic can be reached on 571-272-4023. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Patrick J.D. Santos
February 4, 2005

FRANTZ COBY
PRIMARY EXAMINER